UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

CAROL KANE and BONNIE WILSON,
on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

UNIVERSITY OF ROCHESTER,

Defendant.

Case # 23-CV-6027-FPG

DECISION AND ORDER

INTRODUCTION

Plaintiffs Carol Kane and Bonnie Wilson bring this putative healthcare data privacy class action against the University of Rochester ("Defendant"). *See generally* ECF No. 8. Plaintiffs' claims arise out of Defendant's alleged disclosure, through certain web analytics and marketing tools, of their private health-related information to Facebook. Defendant has moved to dismiss Plaintiffs' amended complaint in its entirety. *See* ECF No. 11. As explained below, Defendant's motion is GRANTED in part and DENIED in part.

BACKGROUND

Defendant operates one of the largest facilities for medical treatment and research in New York state, employing over 26,000 employees and nearly 3,000 clinical researchers. ECF No. 8 ¶ 33.[1] Plaintiff Bonnie Wilson, a citizen of New York, and Plaintiff Carol Kane, a citizen of Florida, have accessed Defendant's website to search for, make appointments with, and communicate with healthcare providers. *Id.* ¶ 37. They allege that, using two web tracking products, the Facebook

[1] Unless otherwise noted, the facts are drawn from the First Amended Complaint, ECF No. 8, and any documents it incorporates by reference or that are "integral" to it. *See Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152–53 (2d Cir. 2002).

Tracking Pixel (the "Pixel") and Conversions Application Programming Interface ("CAPI"), Defendant transmitted their personally identifiable information ("PII") and non-public personal health information ("PHI," collectively with PII, "Private Information") to Facebook without authorization.

I. Facebook's Web Tracking Technology

Facebook operates the world's largest social media platform and generated $117 billion in revenue in 2021, about ninety-seven percent of which came from advertising. *See* ECF No. 8 ¶ 61. Facebook profiles include users' real names, locations, friends, likes, and other communications. *Id.* ¶ 62. Facebook associates that information with personal identifiers, including IP addresses. *Id.* Facebook also tracks non-Facebook users through its marketing products. *Id.* ¶ 63. Facebook sells advertising by highlighting its ability to effectively target users by tracking activity both inside and outside of its own website. *Id.* ¶¶ 64-65.

This tracking allows Facebook to "make inferences about users beyond what they explicitly disclose." *Id.* ¶ 66. Facebook compiles this information into a dataset called "Core Audiences." *Id.* ¶ 67. Advertisers can use this dataset to target their advertisements by using "highly specific filters and parameters." *Id.* They can also build "Custom Audiences," which enable advertisers to reach "people who have already shown an interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website." *Id.* ¶ 69. Finally, Facebook allows advertisers to build "Lookalike Audiences" by "leveraging information from [a] source audience to find new people who share similar qualities." *Id.* In order to build Custom Audiences and Lookalike Audiences, advertisers must provide Facebook with data either by manually uploading customer contact information or using Facebook's "Business Tools." *Id.* ¶ 70.

Facebook's Business Tools, such as the Pixel and CAPI, are designed to "help website owners . . . and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services." ECF No. 8 ¶ 71. These Business Tools are configured to capture certain data by default, such as when a user visits a webpage or that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase. *Id.* ¶ 73. The Business Tools can also track other events. *Id.* ¶ 74. Along with Facebook's "menu of 'standard events' from which advertisers can choose," advertisers can create their own tracking parameters by building a "custom event." *Id.*

The Pixel is a piece of code that "tracks the people and [the] type of actions they take as they interact with a website (or other digital property)," including, among other things, how long they spend on a particular page, which buttons they click, which pages they view, and the text they enter into search bars, chats, or text boxes. *Id.* ¶ 8 (internal quotation marks omitted). When a user accesses a website hosting the Pixel, it directs the user's web browser to send a separate message to Facebook's servers. *Id.* ¶ 76. This separate transmission contains the original request to the host website (known as a "GET" request), along with the additional data that the Pixel has been configured to collect. *Id.*

Among that data would be the user's IP address,[2] device ID, and Facebook ID. *Id.* ¶ 80. A user's Facebook ID is linked to their Facebook profile, which "generally contains a wide range of demographic and other information . . . including pictures, personal interests, work history, relationship status, and other details." *Id.* ¶ 84. When a user accesses a website equipped with the Pixel while logged into Facebook, Facebook receives the "c_user" cookie, which contains the

[2] An IP address identifies a device on the internet and routes internet communications. ECF No. 8 ¶¶ 144-45.

user's unencrypted Facebook ID. *Id.* ¶ 96. When a user has recently logged out of Facebook, Facebook receives the "c_user" cookie as well as the "fr" cookie, which contains an encrypted Facebook ID and browser identifier. *Id.* ¶¶ 98-99. Defendant also used the "_fbp" cookie, which like the "fr" cookie, identifies a user's browser. *Id.* ¶ 100. Because the Facebook ID "uniquely identifies an individual's Facebook account, Facebook—or any other person—can use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile." *Id.* ¶ 84. Facebook uses the fr, _fbp, and c_user cookies to "link to [Facebook IDs] and corresponding Facebook profiles." *Id.* ¶ 108. In other words, if a website visitor is a Facebook user, Facebook will associate the information that it collects through the Pixel with the visitor's name and Facebook profile, and, as a result, their real-world identity. *Id.* ¶ 83.

Defendant's implementation of the Pixel also shared information about user actions with Facebook. For example, when a user selects filters, such as specialty and gender, or enters keywords into the search bar, on Defendant's "Find a Provider" page, those filters and keywords are transmitted to Facebook. ECF No. 8 ¶ 91. While search parameters may be "coded," that does not prevent Facebook from decoding that data to determine that a user searched for, for example, a bone cancer specialist. *See id.* ¶ 92. When a user then selects a physician, the Pixel transmits: "the [user]'s unique and persistent Facebook ID (c_user ID), (ii) the fact that the patient clicked on a specific provider's profile page . . . , (iii) the patient's search parameters (demonstrating that they specifically searched for a female or male doctor and their specialty), and (iv) the [user's] location." *Id.* ¶ 93. Once a user has selected a physician, if the user then proceeded to click the "Schedule an Appointment" button on the physician's profile, the Pixel would transmit that action to Facebook as the "SubscribedButtonClick" event, along with the user's search parameters and Facebook ID. *See id.* ¶ 94.

II. Defendant's Privacy Policies

Defendant sets outs its policies and practices with respect to Private Information in its Privacy Statement and Notice of Privacy Practices (collectively, "Privacy Policies"). *See* ECF No. 8 ¶¶ 112, 113, 115.

In its Privacy Statement, Defendant informs users that it is "committed to protecting your privacy. Any information you provide to us through the URMC website—for example, name, address, and phone number—will never be sold to third parties." *Id.* ¶ 113. Defendant further states that it does not "collect information that would personally identify you unless you choose to provide it. The protected health information that you submit, such as on the appointment request form, is shared only with those people in [Defendant] who need this information to respond to your question or request." *Id.* ¶ 114. Nor does Defendant, according to its Privacy Statement, "share any visitor's protected health information with any third party unrelated to [Defendant], except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization." *Id.*

With respect to marketing services, the Privacy Statement discloses that Defendant uses "Google AdWords remarketing service to advertise URMC services to previous visitors to our site," and that "[a]ny data collected will be used in accordance with our privacy policy and Google's privacy policy." *Id.* ¶ 118. The Privacy Statement also explains Defendant's use of web analytics software, which it uses "to track visitor activity and to better understand how the website can be improved." *Id.* ¶ 120. According to the Privacy Statement, Defendant "does not allow any third party to track or collect personally identifiable information from users," but "[i]f personally identifiable data is collected . . . none of that data will be associated with any other data gathered during the use of this website." *Id.* Defendant "may provide third parties with aggregate statistics

about visitors, traffic patterns and related site information," which, according to the Privacy Statement, "reflect site-usage patterns gathered during visits to our website," but do not "contain behavioral or identifying information about any individual user unless that user has given us permission to share that information." *Id.*

Defendant's Notice of Privacy Practices, on the other hand, explains its legal obligations with respect to Private Information and the permissible uses and disclosures of that information. *See id.* ¶ 115. Among other things, the Notice states that Defendant may use and disclose Private Information for "limited marketing purposes, such as face-to-face communication," but that "[f]or other marketing activities, [it] will obtain your authorization." *Id.* Defendant also acknowledges that it is "required by law to [m]ake sure that medical information that identifies you is kept private" and that patients "have the right to be notified of a breach of . . . unsecured protected health information, with a few limited exceptions." *Id.* ¶ 117.

III. Plaintiffs' Use of Defendant's Web Properties

Plaintiffs Carol Kane and Bonnie Wilson allege that, as a condition of receiving services from Defendant, they disclosed Private Information to Defendant as recently as November 2022 and March 2023, respectively. ECF No. 8 ¶¶ 158, 171. Both Plaintiffs accessed Defendant's website on their phones and computers to receive healthcare services from Defendant, and at Defendant's direction. *Id.* ¶¶ 159, 172. Further, both Plaintiffs used Defendant's website to schedule doctor's appointments. *Id.* ¶¶ 160, 173. Plaintiff Wilson also used Defendant's patient portal (the "Portal"). *Id.* ¶ 172. Throughout the relevant period, both Plaintiffs have used the same devices to maintain and access active Facebook accounts. *Id.* ¶¶ 161, 174.

LEGAL STANDARD

To succeed on a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), the defendant must show that the complaint contains insufficient facts to state a claim for relief that is plausible on its face. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007). A complaint is plausible when the plaintiff pleads sufficient facts that allow the Court to draw reasonable inferences that the defendant is liable for the alleged conduct. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Plausibility "is not akin to a probability requirement." *Id.* Instead, plausibility requires "more than a sheer possibility that a defendant has acted unlawfully." *Id.* "Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Id.* (quotation marks and citation omitted). A pleading that consists of "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555. Nor does a complaint suffice if it tenders "naked assertion[s]" devoid of "further factual enhancement." *Id.* at 557. In considering the plausibility of a claim, the Court must accept factual allegations as true and draw all reasonable inferences in the plaintiff's favor. *Faber v. Metro. Life Ins. Co.*, 648 F.3d 98, 104 (2d Cir. 2011). At the same time, the Court is not required to accord "[l]egal conclusions, deductions, or opinions couched as factual allegations . . . a presumption of truthfulness." *In re NYSE Specialists Sec. Litig.*, 503 F.3d 89, 95 (2d Cir. 2007) (quotation marks omitted).

When deciding a motion under Rule 12(b)(6), a court ordinarily may not rely on matters outside the pleadings. *See* Fed. R. Civ. P. 12(d). For the purposes of this rule, "the complaint is deemed to include any written instrument attached to it as an exhibit or any statements or documents incorporated by reference." *Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152–53 (2d Cir. 2002); *see also* Fed. R. Civ. P. 10(c) ("A copy of any written instrument which is an

exhibit to a pleading is a part thereof for all purposes."). Even where a document is not incorporated by reference, the court may nevertheless consider it where the complaint "relies heavily upon its terms and effect," which renders the document "integral" to the complaint. *Chambers*, 282 F.3d at 152–53.

DISCUSSION

Defendant moves to dismiss Plaintiff's amended complaint in its entirety. In response to Defendant's motion, Plaintiffs have withdrawn their state-law invasion of privacy claim (Count I), one of their federal Wiretap Act claims (Count X), and their Stored Communications Act (Count XI), and Computer Fraud and Abuse Act ("CFAA") claims (Count XII). *See* ECF No. 14 at 13 n.17, 31 n.16. Because Plaintiffs have "expressly abandoned those claims in the face of [Defendant's] motion to dismiss them," the Court dismisses those claims without prejudice. *See Zoulas v. New York City Dep't of Educ.*, 400 F. Supp. 3d 25, 47 (S.D.N.Y. 2019). The Court considers each of Plaintiffs' remaining claims in turn.

I. Plaintiffs' Remaining Federal Wiretap Act Claim (Count IX)

The Court begins with Plaintiffs' only remaining federal law claim, which arises under the Wiretap Act, 18 U.S.C. § 2511(1)(a), (c), (d). Defendant argues that this claim must fail because Defendant was a party to the communication and its purpose in allegedly using the Pixel and CAPI was to analyze how well it was speaking to the public through its website, not to "commit any tort or crime against [Plaintiffs] in particular." ECF No. 11-1 at 25. The Court disagrees. As explained below, Plaintiff has plausibly alleged that Defendant has violated the Wiretap Act.

"In relevant part, the Wiretap Act affords a civil cause of action to an aggrieved individual who has had her oral communications intentionally intercepted by a party to those communications for the purpose of committing a crime or tort." *Caro v. Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010)

(citing 18 U.S.C. §§ 2520, 2511(1), 2511(2)(d)).[3] Courts in the Second Circuit construe this "tort-crime" exception narrowly. *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *3 (S.D.N.Y. July 12, 2018) (quoting *United States v. Jiau*, 734 F.3d 147, 152 (2d Cir. 2013)). Accordingly, to survive a motion to dismiss, a plaintiff invoking this exception must plead sufficient facts to support an inference that the defendant "intercepted the communication for the purpose of a tortious or criminal act that is independent of the intentional act of recording" the communication. *Caro*, 618 F.3d at 99. As the Second Circuit has explained:

> If at the moment he hits "record," the offender does not intend to use the recording for criminal or tortious purposes, there is no violation. But if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation, a civil cause of action exists under the Wiretap Act.

Id.; *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) ("[A]ll authority of which we are aware indicates that the criminal or tortious acts contemplated by § 2511(2)(d) are acts secondary to the acquisition of the communication involving tortious or criminal use of the interception's fruits."). The mere fact that a defendant's conduct results in a crime or a tort is not enough. *Caro*, 618 F.3d at 100 (noting that Congress could have defined the exception in terms of interceptions resulting in a tortious or criminal act but did not).

Plaintiff contends that the tort-crime exception applies because the Health Insurance Portability and Accountability Act ("HIPAA") makes it a crime to, as relevant here, "knowingly and in violation of [the Administrative Simplification provisions of HIPAA] disclose[] individually identifiable health information," or "IIHI," to another person. 42 U.S.C. § 1320d-6(a)(3); *see also id.* § 1320d-6(b) (setting out penalties, including fines and imprisonment). IIHI is:

[3] Plaintiffs do not dispute that Defendant was a party to the communications. *See* ECF No. 14 at 30.

> any information, including demographic information collected from an individual, that (A) is created or received by a health care provider . . . and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Id. § 1320d(6). The Court must therefore determine whether Plaintiff has plausibly alleged (1) that the information at issue is IIHI and, if so, (2) that Defendant intercepted Plaintiffs' communications for the purpose of knowingly disclosing it to another person.

a. IIHI

Plaintiffs allege that Defendant disclosed several categories of information to Facebook: (a) their status as patients; (b) their communications with Defendant through its website and the Portal; (c) medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments; and (d) personally identifiable information including, but not limited to, patients' locations, IP addresses, device identifiers, and individual unique Facebook identifiers. ECF No. 8 ¶ 52. The Court's task here is to determine whether it is plausible that by disclosing this information, Defendant has knowingly disclosed IIHI to Facebook. The Court concludes that it is.

Particularly relevant here are Plaintiffs' allegations regarding the "SubscribedButtonClick" event. Plaintiffs allege that, Defendant has configured the Pixel such that once a user has navigated to a physician's website profile, she may click the "Schedule an Appointment" button or click the physician's phone number to schedule an appointment. *See* ECF No. 8 ¶ 94. When a user does so, Plaintiffs allege, "this action is communicated and shared with Facebook" through the Pixel, and is classified as a "SubscribedButtonClick" event. *Id.* If that user is also logged into Facebook, the Pixel "will transmit the c_user cookie to Facebook, which contains that user's unencrypted

Facebook ID." *Id.* ¶ 96. If the user has recently logged out, the browser sends "a smaller set of cookies," including the "fr" cookie, which contains "an encrypted Facebook ID and browser identifier," which Facebook can use to identify users. *Id.* ¶¶ 98-99. Finally, Plaintiffs allege that Defendant also used the "_fbp" cookie, which "attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user." *Id.* ¶ 100. Facebook can use these cookies to "link [website users] to FIDs and corresponding Facebook profiles." *Id.* ¶ 108.

The Pixel transmits other information too. For example, if a user entered their home address to search for a physician close by, the Pixel would send that search parameter as well. ECF No 8 ¶ 93. The Pixel also transmits the user's IP address, the name and specialty of the physician a user has selected, as well as any other search parameters a user enters, such as gender and specialty. *See id.* ¶¶ 80, 93-95.

The Court finds it plausible that, at the very least, the information transmitted when a user attempts to schedule an appointment with a physician is information that is "received by a health care provider," Defendant, that "relates to . . . the provision of health care to an individual," that is, the appointment the user is attempting to make, and "with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. § 1320d(6). As to that last requirement, Defendant makes much of the fact that the information is transmitted as a "scrambled up jumble of internet code," ECF No. 11-1 at 9, distinguishing it from "actual, confidential medical records." *Id.* While the transmitted data may look "scrambled up" to a human reader, to an individual or entity with the tools to analyze that data, it is perfectly comprehensible. Plaintiff has alleged that, when a user clicks a button on Defendant's website to make an appointment with a specific physician, the website transmits the user's Facebook ID, which can be linked to a specific Facebook profile. This tells Facebook that a particular individual sought

medical care from one of Defendant's providers in a specific specialty. That makes it plausible that by disclosing this information, Defendant disclosed IIHI.

This differs significantly from the information at issue in *Smith v. Facebook*, in which the court concluded that Facebook did not collect "protected health information" and was therefore not subject to HIPAA's strict disclosure requirements. 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017). There, as here, the information transmitted included the contents of certain cookies, along with the user's IP address, and the relevant webpage's URL. *Id.* However, unlike here, the webpages at issue contained "information about treatment options for melanoma, information about a specific doctor, search results related to the phrase 'intestine transplant,' and other publicly available medical information." *Id.* at 954-55. Because those pages contained only "general health information that is accessible to the public at large," the court determined that "nothing about the URLs or the content of the pages located at those URLs, relate[d] 'to the past, present, or future physical or mental health condition of an individual.'" *Id.* at 955 (citing 45 C.F.R. § 160.103)). The court therefore concluded that the information was not "protected health information." *Id.* at 954. Here, however, because Defendant's website transmits data from which it is possible to identify a specific individual who is seeking treatment from a specific physician, the information does relate to the provision of healthcare to an individual. 42 U.S.C. § 1320d(6). And, because Facebook can link this data to a specific user profile, there is a "reasonable basis to believe that the information can be used to identify that individual." *Id*. It would therefore be IIHI for the purposes of section 1320d-6.

The Court acknowledges that at least one district court has rejected the argument that section 1320d-6 could "serve as the basis for the [tort or crime] exception" in a case involving similar allegations. *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 4707184, at *2-3

(N.D. Ill. July 24, 2023) ("*Kurowski II*"). In *Kurowski II*, the plaintiff alleged that the defendant health system secretly deployed "custom analytics scripts," within its website and patient portal, and, in doing so, transmitted, among other things, "personally identifiable patient data" such as "IP addresses, patient cookie identifiers, device identifiers," URLs, and other "unique identifying numbers, characteristics, or codes." *Id.* at *1. The court contrasted the disclosure of this metadata with a situation in which a patient allegedly "entered data relating to her heart issues and high blood pressure in [her healthcare provider's patient portal] and later received advertisements on Facebook, including at least one [] relating to high blood pressure medication." *Id.* at *3 (citing *Doe v. Regents of Univ. of California*, No. 23-CV-598, 2023 WL 3316766, at *2 (N.D. Cal. May 8, 2023). Ultimately, the court concluded that plaintiff had failed to establish that the crime or tort exception applied, as her allegations were "far too vague to allow an inference" that defendant "was actually disclosing IIHI as it is unambiguously defined by HIPAA, rather than just metadata." *Id.* at *3.[4]

That is not true here, though. Here, Plaintiffs have alleged that, when a user schedules an appointment with a provider through Defendant's website, Defendant discloses information that could reasonably identify the user who scheduled the appointment, the provider, and the provider's specialty. It is therefore plausible that Defendant received and then disclosed information relating to the provision of health care that could reasonably identify that user. *See* 42 U.S.C. § 1320d(6). That is enough to make it plausible that Defendant knowingly disclosed IIHI to Facebook through its use of the Pixel.

[4] Notably, the court later granted the plaintiffs leave to amend after concluding that they had sufficiently alleged a violation of section 1320d-6 to invoke the tort-crime exception. *See Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 8544084, at *2 (N.D. Ill. Dec. 11, 2023) ("*Kurowski III*")

b. Defendant's Purpose

The Court must now determine whether it is plausible that Defendant disclosed Plaintiffs' Private Information "for the purpose" of knowingly disclosing IIHI in violation of 42 U.S.C. § 1320d-6. *See Caro*, 618 F.3d at 99. It is.

Plaintiffs allege that Defendant disclosed their Private Information to enhance its marketing efforts. *See e.g.*, ECF No. 8 ¶¶ 22 ("Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook . . . or that their information was stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes."), 152 ("The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits."), 154 ("Upon information and belief, . . . the Pixel was used to 'help [Defendant] understand the success of [its] advertisement efforts on Facebook."). At least one district court has indicated that similar allegations are sufficient to invoke the tort-crime exception. In *Kurowski III*, the court granted the plaintiff's motion for leave to amend their Wiretap Act claim, concluding that they had alleged sufficient facts to "invoke the HIPAA exception-to-the-party exception." *See Kurowski III*, 2023 WL 8544084, at *2. The court concluded that plaintiffs' allegations that the defendant "knowingly transmit[ted]" the information and "[did] so for the purpose of financial gain" was sufficient to invoke the crime-tort exception. *Id.*

This Court likewise concludes that Plaintiffs can invoke the tort-crime exception. Plaintiffs have alleged that Defendant configured the Pixel to collect and disclose, among other things, that a specific user booked an appointment with a specific healthcare provider and the search terms that the user entered to find that provider. *See* ECF No. 8 ¶¶ 91–94. That information, through the c_user cookie, would be associated with a particular Facebook user, that is, with a person's

real-world identity. *See id.* ¶¶ 95–98. They have further alleged that Defendant disclosed this information to enhance its marketing efforts. *See id.* ¶¶ 22, 152, 154. Accordingly, Plaintiffs have plausibly alleged that Defendant's purpose was to commit an act that is punishable as a crime under 42 U.S.C § 1320d-6: knowingly disclosing IIHI without authorization for marketing purposes. *See Kurowski III*, 2023 WL 8544084, at *2.

Defendant may be able to show that, as a factual matter, that they did not intercept Plaintiffs' communications for that purpose. But at this stage of the proceedings, Plaintiffs, without the benefit of discovery, have plausibly alleged that the tort-crime exception applies. *See In Re Grp. Health Plan Litig.*, No. 23-CV-267, 2023 WL 8850243, at *8 (D. Minn. Dec. 21, 2023) (allowing Wiretap Act claim to proceed under tort-crime exception where defendant allegedly used Pixel to enhance marketing efforts). Their Wiretap Act claim may therefore proceed.

II. Breach of Contract (Counts II and V)

The Court now turns to Plaintiffs' state-law claims, beginning with their contract claims. Defendant argues that Plaintiffs have failed to state either a breach of express or implied contract claim. ECF No. 11-1 at 12–14, 16–17. With respect to the express contract claim, Defendant argues that Plaintiffs' claim fails because: (i) Plaintiffs have failed to allege a meeting of the minds with Defendant as to any particular document or set of contract terms; (ii) the HIPAA Notice merely provides notice to patients and potential patients, as required by federal law, of how Defendant can use and disclose protected health information; (iii) the HIPAA notice contains no reciprocal obligations; and (iv) the Privacy Statement limits Defendants' liability and provides that the "sole and exclusive remedy" is to "stop using the service." *Id.* at 12–14. As to the breach of implied contract claim, Defendant argues that it is duplicative of, and therefore subsumed by, the breach of confidence claim. *Id.* at 17. The Court considers each claim in turn.

a. Express Contract (Count II)

Plaintiffs allege that by disclosing certain information through the Pixel and CAPI, Defendant breached its Privacy Policies. ECF No. 8 ¶¶ 112-23, 223-231. Defendant argues that the Notice of Privacy Practices cannot support Plaintiffs' breach of express contract claim because it is simply a notice to patients and potential patients and contains no reciprocal obligations. ECF No. 11-1 at 13. With respect to the Privacy Statement, Defendant argues that the Privacy Statement's exculpatory clause bars Plaintiffs' contract claim. *Id.* at 14.

To make out a viable claim for breach of contract, a "complaint need only allege (1) the existence of an agreement, (2) adequate performance of the contract by the plaintiff, (3) breach of contract by the defendant, and (4) damages." *Harsco Corp. v. Segui*, 91 F.3d 337, 348 (2d Cir. 1996); *see also Miller v. Syracuse Univ.*, 662 F. Supp. 3d 338, 362 (N.D.N.Y. 2023).[5] To form a contract, "there must be a manifestation of mutual assent sufficiently definite to assure that the parties are truly in agreement with respect to all material terms." *Stonehill Capital Mgmt, LLc v. Bank of the West*, 28 N.Y.3d 439, 448 (2016); *Express Indus. and Terminal Corp. v. N.Y. State Dep't of Transp.*, 93 N.Y.2d 584, 589 (1999). "Generally, courts look to the basic elements of the offer and the acceptance to determine whether there is an objective meeting of the minds sufficient to give rise to a binding and enforceable contract." *Id.*

Plaintiff has plausibly pled a breach of express contract claim. Plaintiff alleges that Defendant required them to enter certain information into Defendant's website as a condition of using Defendant's website and receiving healthcare services. ECF No. 8 ¶¶ 223–24. In exchange, Plaintiffs provided this information and paid for medical care. *Id.* ¶ 224. In doing so, Plaintiffs

[5] The parties appear to agree that New York law applies. *See* ECF No. 11-1 at 11–20; ECF No. 14 at 16–27. "Since the parties appear to agree that New York law may properly be applied, and since [Plaintiffs] as the non-moving party advocates for the application of New York law, this Court will dispense with the choice-of-law analysis and apply New York law." *Coe v. Coca-Cola Co.*, No. 22-CV-430, 2023 WL 7524396, at *7 (W.D.N.Y. Nov. 14, 2023).

allege that they entered into contracts with Defendant, by which "Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs . . . if their data had been breached and compromised or stolen." *Id.* ¶ 225. Plaintiffs also allege that they have both used Defendant's website to schedule appointments, as a condition of receiving Defendant's services, disclosed certain Private Information to it. *Id.* ¶¶ 158, 160, 171, 173. Moreover, Plaintiff alleges that Defendant's Privacy Statement makes several express promises that Defendant ultimately breached. For example:

> [1] We do not collect information that would personally identify you unless you choose to provide it. The protected health information that you submit, such as on the appointment request form, is shared only with those people in URMC who need this information to respond to your question or request . . . We do not save protected health information to use for other purposes, nor do we provide it to any other organizations;
>
> [2] We do not collect information that would personally identify you unless you choose to provide it. We also do not share any visitor's protected health information with any third party unrelated to URMC, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization.

ECF No. 8 ¶ 114 (excerpting Privacy Statement); *see also* ECF No. 11-3 at 3, 4 (Privacy Statement attached to Defendant's motion to dismiss). Plaintiff adds that, although the Privacy Statement discloses that Defendant's website uses analytics tools to "better understand how the website can be improved," it conceals its disclosure of Plaintiff's Private Information tool through the Pixel, stating that:

> The website does not allow any third party to track or collect any personally identifiable information from users. If personally identifiable data is collected, (see the Protected Health Information section) none of that data will be associated with any other data gathered during the use of this website[;]

> We may provide third parties with aggregate statistics about our visitors, traffic patterns and related site information. These data reflect site-usage patterns gathered during visits to our website, but they do not contain behavioral or identifying information about any individual user unless that user has given us permission to share that information[;]
>
> [and] [w]e collect information about visitors to our site using "first party cookies" . . . Cookies are never associated with specific personal identities.

ECF No. 8 ¶¶ 120, 122; ECF No. 11-3 at 7, 9. Plaintiff has also plausibly alleged that Defendant violated these terms by disclosing Plaintiffs' Private Information, including Facebook IDs, IP addresses, treatment sought, appointment types, and physicians selected, without consent or authorization. *See* ECF No. 8 ¶¶ 123, 166, 179.

Defendant argues that, to the extent that Plaintiffs allege that the Privacy Statement forms the basis for the parties' contract, that document's exculpatory clause bars Plaintiffs' claim. *Id.* at 14. Under that clause, Defendant asserts, Plaintiff's "sole and exclusive remedy for dissatisfaction with the service is to stop using the service." ECF No. 11-3 at 10 (Privacy Statement's "Limitations of Liability" provision).

"Contractual provisions that 'clearly, directly and absolutely' limit liability for 'any act or omission' are enforceable, 'especially when entered into at arm's length by sophisticated contracting parties.'" *Baidu, Inc. v. Register.com*, 760 F. Supp. 2d 312, 317 (S.D.N.Y. 2010) (quoting *Kalisch-Jarcho, Inc. v. City of New York*, 58 N.Y.2d 377, 384 (1983)). However, New York law recognizes exceptions to this general rule. First, "[s]uch an agreement will be viewed as wholly void . . . where it purports to grant exemption from liability for willful or grossly negligent acts." *Lago v. Krollage*, 78 N.Y.2d 95, 100 (1991). Gross negligence is "conduct that evinces a reckless disregard for the rights of others or 'smacks' of intentional wrongdoing." *Colnaghi,*

U.S.A., Ltd. v. Jewelers Prot. Servs., Ltd., 81 N.Y.2d 821, 823–24 (1993) (citing *Sommer v. Fed. Signal Corp.*, 79 N.Y.2d 540, 554 (1992)). Second, a court will not enforce an exculpatory clause "where a special relationship exists between the parties such that an overriding public interest demands that" the provision "be rendered ineffectual." *Lago*, 78 N.Y.2d at 100.

Plaintiff argues that both of these exceptions apply here because Defendant's "breaches were intentional" and Defendant is Plaintiffs' "healthcare provider," and therefore their "relationship carries duties that go beyond traditional arms-length contract negotiation." ECF No. 14 at 24. The amended complaint alleges that Defendant was aware of its obligations not to disclose their Private Information to third parties without authorization. *See e.g.*, ECF No. 8 ¶¶ 115–17. It also alleges that Defendant specifically promised to share "protected health information [that a patient submits], such as on the appointment request form, . . . only with those people in URMC who need this information to respond to your question or request." *Id.* ¶ 114. But, Plaintiffs allege, Defendant "willfully and intentionally incorporat[ed]" the Pixel and CAPI into its "Website and servers," and, in doing so, "surreptitiously transmitted" their Private Information to Facebook. *Id.* ¶ 21, 22, 28. Finally, they distinguish Defendants' conduct from that of other medical providers who have provide data breach notices to their patients as a result of the "Pixel transmitting PHI to third parties." *Id.* ¶ 21 n.13. This is sufficient to allege that Defendant breached their contract with Plaintiffs intentionally or with gross negligence. Plaintiffs' express contract claim may therefore proceed.

b. Implied Contract (Count V)

Defendant contends that Plaintiffs' breach of implied contract must be dismissed because it is subsumed by their breach of confidence claim (Count VI). ECF No. 11-1 at 16–17. The Court agrees.

Under New York law, a contract implied in fact "may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct." *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 582 (2d Cir. 2006). Such implied contracts are "just as binding as an express contract arising from declared intention." *Jemzura v. Jemzura*, 36 N.Y.2d 496, 504 (1976). Under New York law, the elements of an implied contract claim are identical to those of an express contract claim. *See Wallace*, 2021 WL 1109727, at *10 (citing *Forest Park Pictures v. Univ. TV Network, Inc.*, 683 F.3d 424, 432 (2d Cir. 2012)).

Courts addressing claims of unauthorized disclosure of health-related information have repeatedly rejected implied contract claims in favor of breach of confidence claims. *See e.g.*, *Doe v. Guthrie Clinic, Ltd.*, 519 F. App'x 719, 721 (2d Cir. 2013) (summary order); *MacDonald v. Clinger*, 84 A.D.2d 482, 483, 488 (4th Dep't 1982); *see also Doe v. Community Health Plan-Kaiser Corp.*, 268 A.D.2d 183, 187 (3d Dep't 2000) ("*CHP*") ("[A] plaintiff is entitled to invoke the privilege of professional confidence a breach of which is actionable as a tort even though it arises from a contractual relationship."); *Tighe v. Ginsberg*, 146 A.D.2d 268, 271 (4th Dep't 1989) ("[In *MacDonald*, the court] recognized that the physician-patient relationship creates an implied covenant which when breached is actionable. We declined to characterize the cause of action as a breach of contract. . . .").

Here too, Plaintiffs' implied contract claim here is more properly cast as a tort claim, that is, as a claim for breach of confidence. *See Guthrie Clinic*, 719 F. App'x at 721. Plaintiffs allege that they provided their Private Information to Defendant, a healthcare system, in "exchange for services." ECF No. 8 ¶ 248. From that alleged contractual relationship arose Defendant's duty to maintain the confidentiality of Plaintiffs' Private Information. *See CHP*, 268 A.D.2d at 187. And,

Plaintiffs allege that Defendant breached the implied contract failing to do so. Plaintiffs' implied contract claim is therefore better cast as a tort claim for breach of confidence. *See Guthrie Clinic*, 719 F. App'x at 721.

Plaintiffs point out that at least one district court has permitted both breach of confidence and implied contract claims to survive a defendant health system's motion to dismiss. *See* ECF No. 14 at 15 (citing *Wallace v. Health Quest Sys., Inc.*, No. 20-CV-545, 2021 WL 1109727, at *15 (S.D.N.Y. Mar. 23, 2021)). That decision is of little persuasive value, as it does not purport to analyze whether an implied contract claim is the proper cause of action when a defendant health system has allegedly disclosed private health information without authorization. *See Wallace*, 2021 WL 1109727, at *10–11, 12–13. Whatever conclusion may be implicit in *Wallace*'s outcome, the Court declines to rely on it in the face of clear statements to the contrary from New York and federal courts.

Plaintiffs' implied contract claim is therefore dismissed as duplicative of Plaintiffs' breach of confidence claim.

III. Bailment (Count VII)

Defendant argues that, like Plaintiff's implied contract claim, Plaintiff's bailment claim is subsumed by Plaintiff's breach of confidence claim. ECF No. 11-1 at 16-17. The Court disagrees.

Under New York law, a bailment is the "delivery of personal property for some particular purpose . . . upon a contract express or implied, and that after such purpose has been fulfilled it shall be redelivered to the person who delivered it, or otherwise dealt with according to his directions or kept until he reclaims it." *Herrington v. Verrilli*, 151 F. Supp. 3d 449, 457 (S.D.N.Y. 2001) (quoting *Osborn v. Cline*, 263 N.Y. 434, 437 (1934)). A bailment may be actual or constructive. *Id.* A constructive bailment arises "when the person having possession of property

holds it under such circumstances that the law imposes an obligation to deliver the property to another." *Wallace*, 2021 WL 1109727, at *14 (brackets omitted). Constructive bailments do not require an express assumption of duties, and "may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner." *Id.* (quoting *Ancile Inv. Co., Ltd. v. Archer Daniels Midland Co.*, 784 F. Supp. 2d at 307). To state a claim for breach of a bailment, the bailor must plead that the bailee failed to "exercise care and diligence in protecting and keeping safe" the property. *Id.* at *13.

Unlike implied contract claims, the cases addressing breach of confidence claims are less clear as to whether a plaintiff can also bring a bailment claim. As summarized by one state trial court, "courts have ruled appropriate the tort of breach of confidence, and as inappropriate malpractice, breach of contract, breach of privacy, and prima facie tort." *Fedell v. Wierzbieniec*, 485 N.Y.S.2d 460, 462 (Sup. Ct. Erie Cnty. 1985). Courts have not identified bailment as an example of an "inappropriate" claim in this context. *See e.g.*, *Guthrie Clinic*, 719 F. App'x at 721 (affirming dismissal of implied contract claim); *Tighe*, 146 A.D.2d at 271 (reiterating prior rejection of implied contract as the appropriate cause of action); *MacDonald*, 84 A.D.2d at 483, 487 (affirming dismissal of implied contract and statutory right to privacy claims); This may stem, in part, from the fact that there appears to be no "binding precedent addressing whether a bailment may be created for solely intangible property" like Plaintiffs' Private Information. *Wallace*, 2021 WL 1109727, at *14, and the fact that many of the breach of confidence cases predate the widespread adoption of the internet as a means to seek out healthcare services, as well as the public's increased sensitivity to the security of their digital data. *See e.g.*, *Doe v. Roe*, 190 A.D.2d 463 (4th Dep't 1993).

In any event, Defendant has failed to persuade the Court that Plaintiffs' bailment claim is subsumed by the breach of confidence claim. Instead, it is satisfied that Plaintiffs have plausibly alleged that Defendant owed a duty distinct from the duty of confidentiality, arising out of Defendant's "possession and [] control of Plaintiffs' and Class Members' Private Information." ECF No. 8 ¶ 263. Unlike their implied contract claim, the bailment claim involves breach of a "duty extraneous to the contract" which "exists where the contract results in or accompanies some relation between the parties out of which arises a duty of affirmative care." *MacDonald*, 84 A.D.2d at 804. The relationship of bailor and bailee is one such relationship. *See id.* Moreover, contrary to Defendant's contention, New York cases have not established that no other claim besides breach of confidence is permitted in cases involving the unauthorized disclosure of healthcare information. For example, in *Steiner v. University of Rochester*, the Fourth Department affirmed the trial court's grant of summary judgment as to the plaintiff's breach of confidence and prima facie tort claim. 278 A.D.2d 827, 827 (4th Dep't 2000). Notably, however, the court did not do so on the grounds that a prima facie tort claim was *per se* inappropriate in a case also alleging breach of confidence. *See id.* Instead, the court concluded that the defendants had established that they did not act with intent to harm plaintiff. *See id.* The Court is therefore persuaded that a breach of confidence claim does not subsume a bailment claim, and the Court declines to dismiss that claim on this basis.

Plaintiffs' bailment claim may therefore proceed.

IV. Breach of Confidence (Count VI)

Defendant argues that Plaintiffs fail to state a claim for "breach of physician-patient confidence" because they do not allege that "any actual [University] physician violated their

confidences in any way," but rather "through computer web servers and web browsers over the ethers of the Internet." ECF No. 11-1 at 17-18.

To state a claim for breach of confidence under New York law, a plaintiff must plead that (1) the defendant assumed a duty of confidentiality, (2) the defendant intentionally, knowingly, or negligently breached that duty, and (3) the plaintiff was damaged as a result of that breach. *In re Canon U.S.A. Data Breach Litig.*, 2022 WL 22248656, at *11 (E.D.N.Y. Mar. 15, 2022); *see In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *3 (S.D.N.Y. Feb. 24, 2022) ("New York law recognizes breach of confidence as an independent tort, although one that may only protect a patient's medical information) (citing *Chanko v. Am. Broad. Companies Inc.*, 27 N.Y.3d 46, 53-54 (2016)).

"Although there is no binding precedent extending a claim for breach of confidence to a healthcare provider like [Defendant], this Court, sitting in diversity, is bound to 'predict how the forum state's highest court would decide the issue.'" *Wallace v. Health Quest Sys., Inc.*, No. 20-CV-545, 2021 WL 1109727, at *12 (S.D.N.Y. Mar. 23, 2021) (quoting *DiBella v. Hopkins*, 403 F.3d 102, 111 (2d Cir. 2005)). "This is especially true 'where sufficient precedents exist for' the federal court to make that determination. *Id.* (quoting *Amerex Grp., Inc. v. Lexington Ins. Co.*, 678 F.3d 193, 199-200 (2d Cir. 2012)).

"Sufficient precedent exists here." *Id.* The New York Court of Appeals has stated that a "medical corporation may . . . be liable in tort for failing to establish adequate policies and procedures to safeguard the confidentiality of patient information." *Doe v. Guthrie Clinic, Ltd.*, 22 N.Y.3d 480, 485 (2014). Such claims "provide the requisite incentive for medical providers to put in place appropriate safeguard to ensure protection of patient's confidential information." *Id.* Although the Court found no actionable breach in *Doe*, this "pronouncement is sufficient for the

Court to conclude New York would permit [Plaintiffs] to pursue a breach of confidence claim in this case." *Wallace*, 2021 WL 1109727, at *12 (citing *United States v. Bell*, 524 F.2d 202, 206 (2d Cir. 1975)). According to Defendant, however, Plaintiffs' allegations are too "novel" to state a claim under New York law because the alleged disclosures occurred through cookies, rather than "actual medical records tied to any particular individual on [their] face." ECF No. 11-1 at 18, 19.

While true that the internet—and data transmitted over it—plays a central role in the alleged disclosures here, that, without more, does not make Plaintiffs' claim so novel as to warrant dismissal. Despite Defendant's attempt to mystify Plaintiffs' breach of confidence claim, it is relatively straightforward: Plaintiffs allege (1) that Defendant is a healthcare provider, (2) that Defendant deployed the Pixel and CAPI on its website, (3) that through those tools, Defendant disclosed their Private Information to Facebook, and (4) that they suffered damages as a result. It is conceivable that a medical provider may breach their duty of confidence in this way, even if it involves internet cookies. Nevertheless, as explained below, the Court agrees with Defendants that Plaintiffs have failed to state a breach of confidence claim.

In analyzing breach of confidence claims, New York courts have looked to the state's confidentiality statutes, which require physicians and medical corporations "to protect the confidentiality of patient information gained during the course of treatment," as the source of "scope of the actionable duty which arises between certain healthcare providers . . . and their patients." *Doe v. Community Health Plan-Kaiser Corp.* ("*CHP*"), 268 A.D.2d 183, 187 (3d Dep't 2000), *overruled in part by Guthrie Clinic*, 22 N.Y.3d at 485 (declining to impose absolute liability on medical corporations for breach of confidence). For example, the court in *CHP* noted that N.Y. C.P.L.R. 4504 codifies the "duty to maintain the confidentiality of *patient treatment records*," *id.* at 186 (emphasis added), while N.Y. Public Health Law § 4410(2) prohibits health maintenance

organizations from disclosing "any information acquired *in the course of rendering professional services*." *Id.* (emphasis added); *see also Guthrie Clinic*, 22 N.Y.3d at 465–86 (Rivera, J. dissenting) (discussing New York's public policy to protect the confidentiality of patient medical records) (citing N.Y. Public Health Law § 2803-c(1), (3)(f)). Notably, C.P.L.R. 4504 does not prevent a physician from testifying, for example, that a person was her patient, how many times she attended to her patient, or that the patient visited her and made payments to her. *See Hughson v. St. Francis Hosp. of Port Jervis*, 93 A.D.2d 491, 499 (2d Dep't 1983).

Where courts have permitted breach of confidence claims to proceed, they have hewed closely to the New York's statutory confidentiality provisions. For example, in *Chanko*, the Court of Appeals first noted that the privilege established in C.P.L.R. 4504(a), and therefore the concomitant duty of confidentiality, "covers all information relating to the nature of the treatment rendered and the diagnosis made." 27 N.Y.3d at 53. It then held that the plaintiff estate stated a breach of confidence claim where the complaint alleged that certain defendants disclosed and discussed the decedent's medical condition with cast members of a medical documentary series and allowed the decedent's treatment to be recorded for broadcast. *Id.* at 54.

Federal courts' analysis of the duty of confidentiality has similarly tracked the scope of the New York statutes. In *Wallace*, for example, the court permitted plaintiffs' breach of confidence claim to proceed where they alleged that defendant medical corporation suffered a data breach which resulted in the disclosure of emails and attachments that may have contained, among other things, patient names, provider names, treatment dates, diagnosis information, and health insurance claims information. 2021 WL 1109727, at *1. In *Broden v. Rubinstein*, too, the communications at issue referred to plaintiff's diagnoses, prescriptions, and the defendant

psychiatrist's treatment notes. No. 21 CV 10411, 2022 WL 16925928, at *3 (S.D.N.Y. Nov. 14, 2022).

Defendant, as a healthcare provider, owed a "duty of safekeeping [Plaintiffs'] confidential medical information." *Guthrie Clinic*, 22 N.Y.3d at 485. However, Plaintiffs have not plausibly alleged that the information that Defendant disclosed here is within the scope of that duty because that information is not related to the "treatment rendered" or a "diagnosis made." *Chanko*, 27 N.Y.3d at 53. Although Plaintiffs allege "upon information and belief" that Defendant disclosed their "medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatment," along with personally identifiable information, ECF No. 8 ¶ 52(c)-(d), without additional factual allegations, that is not enough to plausibly state a breach of confidence claim. *Twombly*, 550 U.S. at 557. These sparse allegations stand in stark contrast to, for example, Plaintiffs' detailed account of how Defendants disclosed that an individual attempted to schedule an appointment with a specific provider. *See* ECF No. 8 ¶¶ 89–111 (illustrating ways in which the Pixel discloses that a particular Facebook user has clicked the "Schedule an Appointment" button on a physician's webpage). But that information, without more, does not appear to be within the scope of Defendant's duty of confidentiality. *See Hughson*, 93 A.D.2d at 499. Therefore, disclosing that information to Facebook would not amount to a breach of that duty.

Plaintiffs also include stray references to the Portal. *See e.g.*, ECF No. 8 ¶¶ 4, 6 n.4, 44, 172, 175, 255. Although they allege that Defendant also uses the Pixel to track user activity within the Portal, Plaintiffs do not identify the information from within the Portal that the Pixel transmitted to Facebook. Of the two named Plaintiffs, only Plaintiff Wilson alleges that she used the Portal. *Id.* ¶ 172. But the Court cannot discern from the amended complaint whether Defendant

disclosed information contained within the Portal. Plaintiffs allege that, with respect to both Plaintiff Kane and Plaintiff Wilson, Defendant transmitted the same information: their "Facebook ID, computer IP address, location and information such as treatment sought, appointment type, physician selected, and button/menu selections." *Id.* ¶¶ 166, 179. Neither these nor any other allegations specifically set forth the information within the Portal that Defendant allegedly disclosed to Facebook. So, while it is conceivable that the Pixel transmits information within the scope of Defendant's duty of confidentiality, *see Kurowski III*, 2023 WL 8544084, at *1–2 (discussing allegations that defendant health system transmitted patient communications within her MyChart Portal account), the sparse factual allegations regarding the Portal here fail to nudge Plaintiffs' claim "across the line from conceivable to plausible." *Ashcroft*, 556 U.S. at 680 (quoting *Twombly*, 550 U.S. at 570).

Because Plaintiffs have failed to plausibly allege that the information that Defendant allegedly disclosed to Facebook was within the scope of Defendant's duty of confidentiality, they have failed to state a claim for breach of confidence under New York law. This claim must therefore be dismissed. However, the Court grants Plaintiffs's request for leave to amend their breach of confidence claim to cure the deficiencies that the Court has identified. *See* Fed. R. Civ. P 15(a)(2) ("The court should freely give leave when justice so requires."); *Williams v. Citigroup Inc.*, 659 F.3d 208, 212–13 (2d Cir. 2011) ("[The] permissive standard [of Rule 15(a)(2)] is consistent with our strong preference for resolving disputes on the merits." (internal quotation marks omitted)).

V. Breach of Fiduciary Duty (Count III)

As with Plaintiffs' breach of implied contract claim, Defendant argues that Plaintiffs' fiduciary duty is subsumed by Plaintiff's breach of confidence claim because it is "grounded in the same basic alleged breach [of confidence]." ECF No. 11-1 at 16-17. The Court agrees.

The cases permitting breach of confidence claims make clear that, "the gravamen [of such claims] is fundamentally the breach of the fiduciary duty of confidentiality." *CHP*, 268 A.D.2d at 186; *see also Wallace*, 2021 WL 1109727, at *12 (stating that plaintiff must plead that defendant assumed a duty of confidentiality); *Burton v. Matteliano*, 81 A.D.3d 1272, 1274 (4th Dep't 2011) (recognizing well-established cause of action for breach of fiduciary duty against a physician resulting from the physician's unauthorized disclosure of the patient's medical records); *see also Daly v. Met. Life Ins. Co.*, 4 Misc.3d 887, 892 (Sup. Ct., N.Y. Cnty. 2004) (noting that cause of action for breach of fiduciary duty of confidentiality generally arises out of the unauthorized disclosure of medical records). In other words, whether cast as a "breach of confidence" or a "breach of fiduciary duty of confidentiality," the core of Plaintiffs' claim is the same: that Defendant owed them a duty of confidentiality arising out of the fiduciary relationship between Defendant and Plaintiffs.

In fact, Plaintiffs recognize that the fiduciary relationship that gave rise to Defendant's alleged duty was that of patient and healthcare provider. They argue that Defendant "as a healthcare provider, unquestionably was aware that it owes a fiduciary duty to Plaintiffs to keep their PHI and IIHI secure" and that "Defendant breached this duty by knowingly deploying the Pixel." *See* ECF No. 14 at 18 n.9; *see also* ECF No. 8 ¶¶ 232–38 (breach of fiduciary duty), 254–60 (breach of confidence). In other words, the same alleged breach of the same duty underlies both Plaintiffs' breach of confidence claim and breach of fiduciary duty claim.

The Court therefore dismisses Plaintiffs' breach of fiduciary duty as duplicative of Plaintiffs' breach of confidence claim.

VI. Unjust Enrichment (Count IV)

Defendant argues that Plaintiffs' unjust enrichment claim must be dismissed because they have failed to allege an actual detriment. ECF No. 11-1 at 14-16. The Court disagrees.

To state a claim for unjust enrichment under New York law, "the plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." *Wallace*, 2021 WL 1109727, at *11 (quoting *Georgia Malone & Co., Inc. v. Reider*, 19 N.Y.3d 511, 516 (2012)). "The essence of such a claim is that one party has received money or a benefit at the expense of another." *Kaye v. Grossman*, 202 F.3d 611, 616 (2d Cir. 2000). The existence of either an express or implied contract precludes recovery on a quasi-contractual claim like unjust enrichment. *Nakamura v. Fujii*, 253 A.D.2d 387, 390 (1st Dep't 1998). But "where a bona fide dispute exists as to the existence of [a] contract, the plaintiff may proceed on both breach of contract and quasi-contract theories." *Id.*

Plaintiffs have plausibly alleged a claim for unjust enrichment. Plaintiffs claim that they used Defendant's website to make doctor's appointments and "reasonably expected that [their] communications with Defendant via the Website were confidential, solely between [themselves] and Defendant, and that such communications would not be transmitted to or intercepted by a third party." ECF No. 8 ¶¶ 162, 175. However, by deploying the Pixel, Defendant did in fact transmit certain Private Information to Facebook. *Id.* ¶¶ 152-157, 166, 179. As a result, Plaintiffs allege, they were denied the benefit of the bargain, that the value of their Private Information has diminished, and there is a "continued and ongoing risk" to that Private Information. *Id.* ¶¶ 169,

182. Defendant, on the other hand, was enriched "in the form of enhanced advertising services and more cost-efficient marketing on Facebook." ECF No. 8 ¶¶ 152-157, 166, 179.

Without more robust factual allegations, the alleged diminution in value of Plaintiff's Private Information is insufficient to plausibly plead that Defendant's enrichment was at Plaintiffs' expense. *See Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 36–37 (2d Cir. 2017) (summary order). Plaintiffs correctly point out that *Mount* addressed this theory in the context of web browsing history, not private health-related information. The Court agrees both that the data Defendant disclosed differ from the browsing history at issue in *Mount* and that it may have market value. *Klein v. Facebook, Inc.*, 580 F. Supp. 3d 743, 803-04 (N.D. Cal. 2022) (collecting cases recognizing that plaintiffs who lose personal information have suffered an economic injury). Even so, because Plaintiffs are, in part, proceeding on the theory that the Defendant's disclosure of their Private Information reduced the value of that information, they must still allege "specific loss or deprivation of opportunity to profit from that information," *id.*, in order to state a claim for unjust enrichment. Plaintiffs' allegations, like those in *Mount*, are too general to survive a motion to dismiss.

Nevertheless, Plaintiff's unjust enrichment claim may proceed because they also allege that Defendant's disclosure of their Private Information denied them the benefit of their bargain. Along with the diminution in value of their Private Information, Plaintiffs allege that they lost the benefit of the bargain, claiming that, for example, they have paid Defendant for services that they would not have had they known about Defendant's disclosure of their Private Information. *See* ECF No. ¶¶ 169, 182, 284-85. These allegations "plead the 'essence' of a claim for unjust enrichment." *Wallace*, 2021 WL 1109727, at *11 (citing *Kaye*, 202 F.3d at 616); *see also Schneider v. Colgate-Palmolive Co.*, No. 22-CV-1294, 2023 WL 4009099, at *9 (N.D.N.Y. June 15, 2023) (concluding

that allegations that plaintiffs were denied benefit of the bargain were sufficient to survive motion to dismiss). Plaintiff's unjust enrichment claim is therefore sufficient to survive Defendant's motion to dismiss.

Moreover, because Defendant disputes whether a contract exists, Plaintiffs "may proceed with their claims for both [breach of contract] and unjust enrichment." *Wallace*, 2021 WL 1109727, *11 (citing *Nakamura*, 253 A.D.2d at 390).

VII. General Business Law § 349 (Count VIII)

Defendant argues that Plaintiffs' claim under General Business Law ("GBL") § 349 must fail because they have failed to allege (1) that they made any purchase through Defendant's website or otherwise paid to use it, (2) a material deception, (3) an injury that resulted from that deception, or (4) that they reviewed Defendant's Privacy Policies. ECF No. 11-1 at 21. Defendant also argues that Plaintiffs' allegations of "unfair," rather than deceptive, acts or practices cannot serve as a basis for a GBL § 349 claim. *Id.* at 20. None of Defendant's arguments warrant dismissal.

GBL § 349(a) makes unlawful all "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [New York]." *Himmelstein, McConnel, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., Inc.*, 37 N.Y.3d 169, 176 (2021), *rearg. den.*, 37 N.Y.3d 1020 (2021). To state a claim under GBL § 349, a plaintiff must allege that: (i) "the defendant's conduct was consumer-oriented"; (ii) 'the defendant's act or practice was deceptive or misleading in a material way"; and (iii) "the plaintiff suffered an injury as a result of the deception." *Id.* (citing GBL § 349(h)). New York courts define the term "deceptive acts or practices" objectively, as "representations or omissions, limited to those likely to mislead a reasonable consumer acting reasonably under the circumstances." *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 26 (1995); *see also Fero*

v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 775 (W.D.N.Y. 2016). Whether a particular act or practice is deceptive is usually a factual question. *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 775 (W.D.N.Y. 2016).

a. Consumer-Oriented Conduct

To start, Plaintiffs have plausibly alleged that the Privacy Policies are consumer-oriented conduct. Plaintiffs allege that they used Defendant's website to receive healthcare services and schedule doctor's appointments. ECF No. ¶¶ 159, 160, 172, 173. That is enough to plead that Defendant's Privacy Policies were consumer-oriented conduct. *See Wallace*, 2021 WL 1109727, at *15 (holding that privacy statements posted on healthcare system's website were consumer-oriented conduct for purposes of GBL § 349).

b. Deceptive or Misleading Acts or Practices

Plaintiffs have also plausibly alleged that Defendants' representations as to its use of analytics and personally identifiable information were "likely to mislead a reasonable consumer acting reasonably under the circumstances." *Oswego Laborers' Local 214 Pension Fund*, 85 N.Y.2d at 26; *see also Fero*, 236 F. Supp. 3d at 776-77 (declining to dismiss GBL § 349 claim grounded in defendant's representations regarding data security). Defendants' Privacy Statement discloses that Defendant's website uses "Web analytics software to track visitor activity and to better understand how the website can be improved." ECF No. 11-3 at 9. It further states that, "the website does not allow any third party to track or collect personally identifiable information from users" and that if such information is collected, "none of that data will be associated with any other data gathered during the use of the website." *Id.* Plaintiffs have plausibly alleged, however, that because the Facebook Pixel transmits a user's Facebook ID, the fact that that user clicked on a specific provider's profile, search parameters (including, for example, a physician's gender and

specialty), and the user's location. *See* ECF No. 8 ¶ 93. Although some of this information is encoded, Plaintiff has plausibly alleged that it is personally identifiable because a Facebook ID is linked to a user's Facebook profile, which identifies that user by name. *Id.* ¶¶ 82-84. Facebook is therefore able to access the corresponding Facebook profile and, in doing so, learn that, for example, that user searched for a physician specializing in bone cancer. *See id.* ¶¶ 81-99. Accordingly, Plaintiffs have plausibly alleged that, despite Defendant's statement that no personally identifiable information "will be associated with any other data gathered during the use of the website," personally identifiable data such as a user's Facebook ID and IP address are, in fact, associated with, for example, the parameters of a user's provider search. That is enough to make it plausible that Defendant's representation would mislead a reasonable consumer. *See Fero*, 236 F. Supp. 3d at 777.

c. Injury

With respect to injury, Plaintiffs allege that they have suffered (1) financial losses related to payments they would not have made to Defendant had they known of Defendant's disclosures, (2) lost control over the value of their personal information, and (3) other harm resulting from the unauthorized use or threat of unauthorized use of their personal information, including for unwanted solicitations or marketing. ECF No. 8 ¶ 285. Defendant argues that Plaintiffs have not alleged an injury "as to themselves personally," instead presenting only a "bare [claim] for alleged deception as to the public at large." ECF No. 11 at 22. The Court disagrees.

Plaintiffs' allegation that they suffered financial losses related to payments they would not have otherwise made sufficiently alleges an injury in the form of "lost benefit of the bargain." "Lost benefit of the bargain is a viable theory of injury" under GBL § 349. *See Wallace*, 2021 WL 1109727, at *6 (citing *Orlander v. Staples, Inc.*, 802 F.3d 289, 299-302 (2d Cir. 2015)); *see also*

In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, (N.D. Cal. 2016) (relying on *Orlander* to conclude that lost benefit of the bargain is sufficient to allege an injury under GBL § 349). In *Orlander v. Staples, Inc.*, the Second Circuit concluded that the plaintiff sufficiently alleged an injury stemming from a misleading practice when he alleged that he would not have purchased a two-year service plan had he known that the defendant "intended to decline to provide him any services in the first year" of the plan. 802 F.3d at 301. Here too, Plaintiffs allege that they "never would have . . . purchased Defendant's services had they known or been told that Defendant shared their confidential and sensitive Private Information with Facebook." ECF No. 8 ¶ 284.

Plaintiff's allegations that they would not have provided their Private Information to Defendant had they known of Defendant's practices likewise sufficiently pleads that they were denied the benefit of the bargain. In *Wallace*, the court concluded that the plaintiffs had plausibly plead injury for the purposes of GBL § 349 where they alleged that they "provided their Private Information to defendant with the reasonable expectation and mutual understanding that defendant . . . would comply with their obligations to keep" that information "confidential and secure from unauthorized access." 2021 WL 1109727, at *6. Plaintiffs here likewise allege that (1) in light of Defendant's Privacy Policies and legal obligations, they had "reasonable expectations of privacy" in the information they provided to Defendants and (2) had they known that Defendant shared that information with Facebook they "never would have provided" that information to Defendant. ECF No. 8 ¶¶ 271, 277-78, 284. That too is enough to plausibly allege that Plaintiffs were denied the benefit of the bargain. *Wallace*, 2021 WL 1109727, at *6.

Accordingly, Plaintiffs have adequately alleged that they suffered an injury for the purposes of GBL § 349.

d. Causation

Defendant also argues that Plaintiffs' GBL § 349 claim must be dismissed because Plaintiffs have failed to allege that they viewed the Privacy Policies. The Court disagrees.

It is true that a plaintiff must generally state in her complaint that she "has seen the misleading statements of which [she] complains." *O'Neill v. Standard Homeopathic Co.*, 346 F. Supp. 3d 511, 530 (S.D.N.Y. 2018) (quoting *Goldemberg v. Johnson & Johnson Consumer Companies, Inc.*, 8 F. Supp. 3d 467, 480 (S.D.N.Y. 2014) (citing *Gale v. Int'l Bus. Machs. Corp.*, 9 A.D.3d 446 (2004))). But even without such an express allegation, where a plaintiff describes in detail the allegedly misleading and deceptive statements, "the reasonable inference to be drawn" is that she "saw the misleading statements, and, as a result of such, purchased the [product] at issue." *Dash v. Seagate Tech. (U.S.) Holdings, Inc.*, 27 F. Supp 3d 357, 361 (E.D.N.Y. 2014)

Here, Plaintiffs describe the relevant provisions of Defendant's Privacy Policies in detail, *see e.g.*, ECF No. 8 ¶¶ 114, 120, and state that they trusted that the Private Information that they provided to Defendant would be "safeguarded according to Defendant's policies and state and federal law." *Id.* ¶¶ 162-63, 175-76. The reasonable inference is that Plaintiffs saw the Privacy Policies and were deceived into providing their Personal Information to Defendant. *See O'Neill*, 346 F. Supp. 3d at 531; *Dash*, 27 F. Supp. 3d at 361.D.N.Y. 2014). Plaintiffs have therefore sufficiently pled causation for the purposes of GBL § 349.

e. Conclusion

Because Plaintiffs have plausibly alleged that Defendant's conduct was consumer oriented, that Defendant's promises with respect to data privacy were deceptive and misleading in a material way, and that they suffered an injury as a result, Plaintiffs have stated a claim under GBL § 349. The Court therefore denies Defendant's motion to dismiss this claim.

CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss, ECF No. 11, is GRANTED in part and DENIED in part. Plaintiffs' invasion of privacy (Count I), breach of fiduciary duty (Count III), implied contract (Count V), breach of confidence (Count VI), Wiretap Act (18 U.S.C. § 2511(3)(a)) (Count X), Stored Communications Act (Count XI), and CFAA (Count XII) claims are DISMISSED.

Plaintiffs' express contract (Count II), unjust enrichment (Count IV), bailment (Count VII), GBL § 349 (Count VIII), and Wiretap Act (18 U.S.C. § 2511(1)) (Count IX) claims may proceed as pled.

Plaintiffs' request for leave to amend their complaint is GRANTED. Plaintiffs may file an amended complaint to cure the pleading deficiencies identified above no later than April 18, 2024. If Plaintiff files an amended complaint, Defendant must move or otherwise respond by May 9, 2024. If Plaintiff does not file an amended complaint, Defendant must answer the remaining claims by May 9, 2024.

IT IS SO ORDERED.

Dated: March 19, 2024
Rochester, New York

HON. FRANK P. GERACI, JR.
United States District Judge
Western District of New York